

IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-32. (Canceled).

33. (Currently Amended) A method for managing a computer system on a network, the computer system including a computing node located on the network side of a network connection on the network and one or more mobile devices located on a user's side of the network connection on the network, comprising:

running a discovery program on the network side of the network connection, the discovery program comprising:

scanning the network based on a scan profile defining at least one parameter for connecting to at least one of domains, computing nodes, and mobile devices;

detecting at least one domain on the network in accordance with the parameters defined in the scan profile,

detecting at least one computing node within the detected domain in accordance with the parameters defined in the scan profile, and

connecting to at least one of the detected computing nodes in accordance with the parameters defined in the scan profile,

detecting, using [[a]] the discovery program, one or more mobile devices ~~on the network that are~~ connected to the detected computing node;

detecting, using [[a]] the discovery program, one or more mobile devices ~~on the network~~ that were previously, but are not currently, connected to the detected computing node;

determining information regarding at least one of the detected mobile devices based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure, a database entry, the presence of an executable program and attributes associated with a mobile device or resource; and

using the determined mobile device information to manage security of the computer system from the network side of the network connection.

34. (Cancelled)

35. (Original) The method of claim 33, wherein the discovery program is run in at least one of a remote central station or a local computing node.

36. (Previously Presented) The method of claim 33 further including grouping the detected mobile devices or resources by type and other attribute.

37. (Currently Amended) The method of claim ~~[[34]]~~ 33, wherein the scan profile contains information regarding at least one of network, domain, IP address, netmask, and computer identity to be scanned, time of synchronization and device connection.

38. (Currently Amended) The method of claim ~~[[34]]~~ 33, wherein the scan profile contains information regarding at least one of network, domain, IP address, netmask, and computer identity not to be scanned.

39. (Currently Amended) The method of claim ~~[[34]]~~ 33, wherein the results of scanning are analyzed and populated and stored and displayed to the users.

40. (Previously Presented) The method of claim 33, wherein the determined mobile device information includes at least one of device type, device identity, synchronization software type, synchronization software availability, synchronization software location, synchronization software version number, previous synchronization information, data and time of last synchronization, the type of device used during previous synchronization, synchronization ID, device owner information, type of applications and files installed or used on the mobile device, file size, file name, file attribute, manufacturer information, time of all completed and

incomplete synchronization and data access and connections performed, type of data and information transferred to and from a mobile device and a resource.

41. (Previously Presented) The method of claim 33, further comprising at least one of locking and denying access to an unauthorized mobile device attempting to access the computer system.

42. (Previously Presented) The method of claim 33, further comprising a step of locking an authorized mobile device attempting to access the network.

43. (Previously Presented) The method of claim 42, wherein the locking step comprises transmitting security software to the mobile device.

44-45. (Cancelled)

46. (Previously Presented) The method of claim 33, wherein the step of running the discovery program results in detection of at least one of a device type, connection profile, or location of at least one of the mobile devices and resource devices.

47. (Currently Amended) A system for managing a computer system on a network, the computer system including a computing node located on network side of a network connection on the network and one or more mobile devices located on a user's side of the network connection on the network, comprising:

means for running a discovery program on the network side of the network connection, the means for running the discovery program comprising:

means for scanning the network based on a scan profile defining at least one parameter for connecting to at least one of domains, computing nodes, and mobile devices;

means for detecting at least one domain on the network in accordance with the parameters defined in the scan profile,

means for detecting at least one computing node within the detected domain in accordance with the parameters defined in the scan profile, and

means for connecting to at least one of the detected computing nodes in accordance with the parameters defined in the scan profile,

means for detecting, using [[a]] the discovery program, one or more mobile devices ~~on the network~~ that are connected to the detected computing node;

means for detecting, using [[a]] the discovery program, one or more mobile devices ~~on the network~~ that were previously, but are not currently, connected to the detected computing node;

means for determining information regarding at least one of the detected mobile devices-based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure, a database entry, the presence of an executable program and attributes associated with a mobile device or resource; and

means for using the determined mobile device information to manage security of the computer system from the network side of the network connection.

48. (Cancelled)

49. (Previously Presented) The system of claim 47, wherein the discovery program is run in at least one of a remote central station or a local computing node.

50. (Previously Presented) The system of claim 47, further comprising a means for grouping the detected mobile devices or resources by type and other attribute.

51. (Currently Amended) The system of claim [[48]] 47, wherein the scan profile contains information regarding at least one of network, domain, IP address, netmask, and computer identity to be scanned, time of synchronization and device connection.

52. (Currently Amended) The system of claim ~~[[48]]~~ 47, wherein the scan profile contains information regarding at least one of network, domain, IP address, netmask, and computer identity not to be scanned.

53. (Previously Presented) The system of claim 47, wherein the results of scanning are analyzed and populated and stored and displayed to the users.

54. (Previously Presented) The system of claim 47, wherein the determined mobile device information includes at least one of device type, device identity, synchronization software type, synchronization software availability, synchronization software location, synchronization software version number, previous synchronization information, data and time of last synchronization, the type of device used during previous synchronization, synchronization ID, device owner information, type of applications and files installed or used on the mobile device, file size, file name, file attribute, manufacturer information, time of all completed and incomplete synchronization and data access and connections performed, type of data and information transferred to and from a mobile device and a resource.

55. (Previously Presented) The system of claim 47, further comprising a means for locking an unauthorized mobile device attempting to access the computer system.

56. (Previously Presented) The system of claim 47, further comprising a means for denying access to an unauthorized mobile device attempting to access the computer system.

57. (Previously Presented) The system of claim 47, further comprising a means for locking an authorized mobile device attempting to access the network.

58. (Previously Presented) The system of claim 57, wherein the locking step comprises transmitting security software to the mobile device.

59. (Cancelled)

61. (Previously Presented) The system of claim 47, wherein the step of running the discovery program results in detection of at least one of a device type, connection profile, or location of at least one of the mobile devices and resource devices.